m	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$L(m)$	29	17	3	22	45	56	52	59	48	13	21	4	7	36	16	30

m	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62
$L(m)$	40	11	28	61	38	2	18	15	37	62	1	39	31	51	57

При помощи этой таблицы можно решить задачу Киркмана для 63 школьниц, так как в таблице содержатся тройки с нулевым элементом, а добавляя 1, можно получить все тройки, которых будет $(63/3) \times ((63 - 1)/2) = 651$.

Вывод

Таким образом, можно сделать вывод, что удобно использовать логарифм Зеха – Якоби для нахождения троек Штейнера и последующего решения задачи Киркмана о школьницах. Сначала составляется таблица степеней простейшего многочлена, затем по этой таблице можно составить таблицу перестановок логарифма Зеха – Якоби, из нее получить тройки Штейнера и, соответственно, решение задачи Киркмана. Данный метод значительно упрощает нахождение троек Штейнера, которые используются в совершенных шифрах.

АВТОМАТИЗАЦИЯ МАТЕМАТИЧЕСКОГО АЛГОРИТМА РАСШИРЕНИЯ БИНАРНЫХ ПОЛЕЙ

Е. А. Букина, О. О. Ванцева, М. Ю. Филиппов, Кр. Л. Геут
(Екатеринбург, УрГУПС, prosto-bukina@mail.ru)

Научно-исследовательский проект посвящен автоматизации математического алгоритма расширения бинарных полей и построения неприводимых многочленов больших степеней вида 2^n, используемых для работы регистров сдвига, реализации криптографических алгоритмов и решения других задач кодирования и защиты информации.

В последние годы повсеместно и с большой интенсивностью ведутся работы по созданию и применению различных автоматичес-

ких систем дискретного действия для переработки информации. Они лежат в основе быстродействующих цифровых вычислительных машин, автоматических устройств для управления объектами и систем, моделирующих деятельность живого организма (так называемых роботов). Производство кибернетических автоматов растет быстрыми темпами, непрерывно расширяются области их применения [1].

Необходимым условием правильной работы системы является обеспечение безопасности и защиты каналов связи. Особое значение это имеет для транспортных систем, в том числе и железнодорожных, так как, в отличие от стационарных систем связи, специфика обмена информацией на транспорте состоит в невозможности препятствия физического проникновения злоумышленника в канал связи. Важной задачей является удаленное управление транспортными средствами с защитой информации от несанкционированного доступа к управлению, примером такого управления являются замки автомобильной сигнализации, отслеживание положения локомотива, связь диспетчера с машинистом, оформление и проверка проездных документов [2; 3].

В предыдущей работе [4] было построено бинарное дерево посредством поликвадратичного расширения операции A. Причем движение по такому дереву возможно как «сверху вниз» с помощью операции A, так и «снизу вверх», применив обратную операцию «антиA». Рассмотрим этот процесс на примере.

Для примера возьмем симметричный многочлен

$$x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^8 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

Найдем его «многочлен-напарник», у которого корень имеет сдвиг = 1, т. е. $x + 1$:

$$(x + 1)^{16} + (x + 1)^{15} + (x + 1)^{14} + (x + 1)^{13} + (x + 1)^{12} + (x + 1)^{11} +$$
$$+ (x + 1)^8 + (x + 1)^5 + (x + 1)^4 + (x + 1)^3 + (x + 1)^2 + (x + 1) + 1 =$$
$$= (x^{16} + 1) + (x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 +$$
$$+ x^4 + x^3 + x^2 + x + 1) + (x^{14} + x^{12} + x^{10} + x^8 + x^6 + x^4 + x^2 + 1) +$$
$$+ (x^{13} + x^{12} + x^9 + x^8 + x^5 + x^4 + x + 1) + (x^{12} + x^8 + x^4 + 1) +$$
$$+ (x^{11} + x^{10} + x^9 + x^8 + x^3 + x^2 + x + 1) + (x^8 + 1) + (x^5 + x^4 + x + 1) +$$
$$+ (x^4 + 1) + (x^3 + x^2 + x + 1) + (x^2 + 1) + (x + 1) + 1.$$

И после сокращений получаем:

$$x^{16} + x^{15} + x^{10} + x^9 + x^7 + x^5 + x^3 + x^2 + 1.$$

Перемножаем эти многочлены.

Результат: $x^{32} + x^{24} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{14} + x^{13} + x^{11} + x^{10} + x^9 + x^6 + x^4 + x^3 + x + 1$.

Затем «подбираем» многочлен, из которого посредством операции A и получился многочлен 32-й степени:

$$(x^{32} + x^{16}) + (x^{24} + x^{20} + x^{16} + x^{12}) + (x^{22} + x^{21} + x^{20} + x^{19} + x^{14} + x^{13} + x^{12} + x^{11}) + (x^{20} + x^{18} + x^{12} + x^{10}) + (x^{12} + x^{10} + x^8 + x^6) + (x^{10} + x^9 + x^6 + x^5) + (x^8 + x^4) + (x^6 + x^5 + x^4 + x^3) + (x^4 + x^2) + (x^2 + x) + 1.$$

После сворачивания степеней получаем искомый многочлен: $x^{16} + x^{12} + x^{11} + x^{10} + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ [5].

Данные расчеты были автоматизированы в программе Microsoft Office Excel.

Сначала в программе заполняется таблица степеней каждого многочлена 16-й степени по «треугольнику Паскаля». Единица соответствует наличию степени (рис. 1).

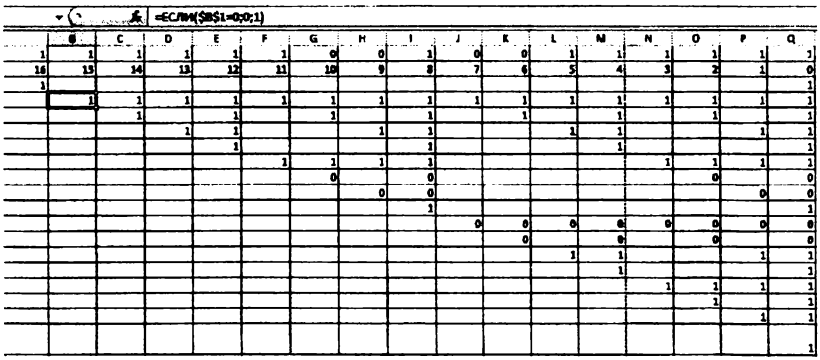

Рис. 1. Представление треугольника Паскаля

Далее суммируем единицы в каждом столбце. И проверяем четность полученных значений. Таким образом, находится «многочлен-напарник».

Следующим этапом мы перемножаем два многочлена: исходный и его напарник. Для этого используем формулу, представленную в строке формул на рис. 2.

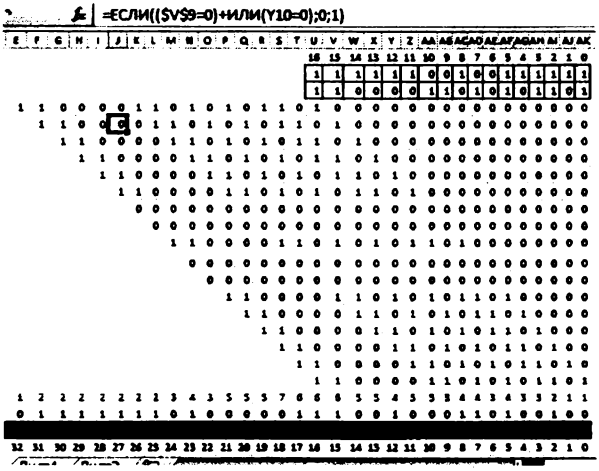

Рис. 2. Произведение многочленов

Результатом этой операции является многочлен 32-й степени. Далее «подбираем» многочлен, из которого посредством операции A и получился многочлен 32-й степени. Для нахождения конечного результата счет идет от старшей степени. Каждый многочлен раскладывается по степеням. При отсутствии какой-либо степени значения записываются из верхней строки. При наличии – значение считается по формуле, представленной в строке формул на рис. 3.

В итоге мы получили искомый многочлен 16-й степени, выведенный из многочлена 32-й степени посредством операции A. Аналогично рассчитываются остальные многочлены, в дальнейшем составляющие бинарное дерево.

Таким образом, в результате исследований был разработан и автоматизирован математический алгоритм расширения бинарных полей. В ходе работы посчитаны неприводимые многочлены больших степеней вида 2^n путем применения операции A.

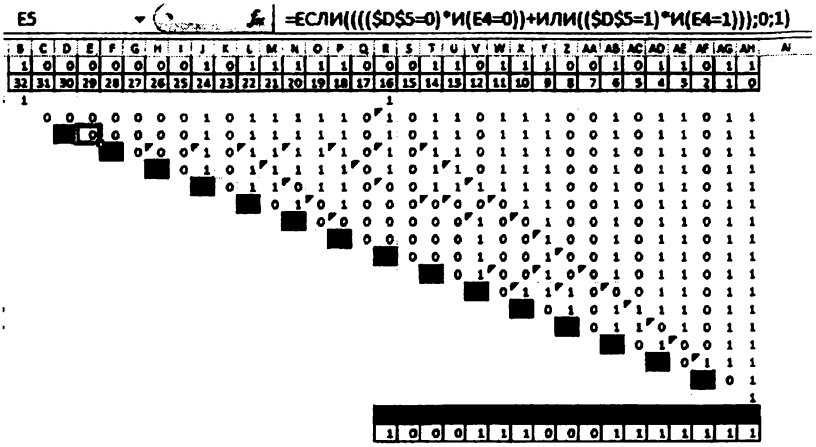

Рис. 3. Свертка операции *A*

Сгенерированные многочлены могут найти свое применение в работе регистров сдвига, конечных автоматов, при реализации криптографических алгоритмов, теории кодирования и защиты информации.

Библиографические ссылки

1. *Болотов А. А.*, *Гашков С. Б.*, *Фролов А. Б.* Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. М. : КомКнига, 2006. 360 с.

2. *Болотов А. А.*, *Гашков С. Б.*, *Фролов А. Б.* Элементарное введение в эллиптическую криптографию : Протоколы криптографии на эллиптических кривых. М. : КомКнига, 2006. 280 с.

3. *Глуско К. Л.*, *Титов С. С.* Нормальные базисы и дерево квадратичных расширений бинарных полей // Некоторые актуальные проблемы современной математики и математического образования : Герценовские чтения – 2012 : материалы науч. конф. СПб. : БАН, 2012. 226 с.

4. *Букина Е. А.*, *Ванцева О. О.*, *Филиппов М. Ю.*, *Геут Кр. Л.* Построение бинарного дерева посредством поликвадратичного расширения // Математическое моделирование системных взаимодействий в прикладных исследованиях : сб. науч. тр. Екатеринбург : УрГУПС, 2013. Вып. 13(196). С. 73–78.

5. *Титов С. С., Торгашова А. В.* Генерация неприводимых многочленов, связанных степенной зависимостью корней // Докл. Том. гос. ун-та систем управления и радиоэлектроники. Томск : ТУСУР, 2010. Вып. № 2 (22), ч. 1. С. 310–318.

ПОСТРОЕНИЕ НЕПРИВОДИМЫХ МНОГОЧЛЕНОВ ПРОСТЫХ ПОРЯДКОВ

Кр. Л. Геут, С. С. Титов
(Екатеринбург, УрГУПС, gluskokrl@rtural.ru)

Неприводимые многочлены нашли свое применение в различных областях математики, информационной техники и защите информации. Неприводимым называется многочлен с коэффициентами из $GF(q)$ (т. е. многочлен над конечным полем $GF(q)$), не являющийся произведением двух многочленов меньшей ненулевой степени.

Неприводимые многочлены, с помощью которых фактически строятся поля Галуа, являются аналогом простых чисел в натуральном ряду. Нахождение их, как и простых чисел, производится подбором и требует больших затрат вычислительных мощностей сверхбыстродействующих ЭВМ. Использование свойств неприводимых многочленов позволяет максимизировать эффективную компьютерную реализацию арифметики в конечных полях, что имеет особое значение для криптографии и теории кодирования. Так, например, реализация электронной цифровой подписи на эллиптических кривых в полях большой степени является актуальной задачей электронной коммерции.

Среди неприводимых многочленов особый интерес представляют примитивные многочлены, т. е. такие, корни которых являются примитивными (или порождающими) элементами поля разложения этого многочлена. Примитивные элементы являются основаниями дискретных логарифмов, находящих широкое применение в асимметричной криптографии [1; 2].